WHAT IS CLAIMED

1. A mobile device operable in a mobile telecommunications network, comprising:

a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

an operating system operable to execute an intrusion detection application stored in the memory module.

2. The mobile device according to claim 1, wherein the operating system further comprises a network stack comprising a protocol driver, a media access control driver, the intrusion detection application comprising an intermediate driver bound to the protocol driver and the media access control driver.

3. The mobile device according to claim 1, wherein the intrusion detection application further comprises an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file and pass the signature file to the associative process engine, the associative process engine operable to analyze a data packet with the signature file.

4. The mobile device according to claim 1, further comprising a storage media, the storage media operable to maintain a database of a plurality of signature files therein.

5. The mobile device according to claim 3, wherein the intrusion detection application identifies a correspondence between the signature file and a data packet, a determination that the data packet is intrusion-related made upon identification of the correspondence.

6. The mobile device according to claim 3, wherein the signature file comprises a directive that defines a process to be executed by the processor upon a determination that the data packet is intrusion-related.

7. The mobile device according to claim 5, wherein the directive comprises machine readable instructions that, when executed by the processor, cause the mobile device to log the data packet in a database.

8. The mobile device according to claim 1, wherein the intrusion detection application performs host-based intrusion detection by monitoring application logs of applications running on the mobile device.

9. The mobile device according to claim 1, wherein the intrusion detection application is operable to identify an event related to an intrusion of the mobile device, the mobile device operable to provide event-data related to the intrusion to a management node of the network.

10. The mobile device according to claim 9, wherein the management node is a mobile telecommunication network switching system.

11. A node of a network for managing an intrusion detection system, the node comprising:

a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input defining a network-exploit rule and convert the text-file input into a signature file comprising machine-readable logic representative of an exploit-signature, the node operable to transmit the signature file to a mobile device over a radio frequency link.

12. The node according to claim 11, wherein the radio frequency link is terminated by the mobile device and a base transceiver station of a mobile communications network.

13. The node according to claim 11 further comprising at least one of a visitor location register and a home location register.